**IN THE UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

| | | |
|---|---|---|
| UNITED STATES | ) | |
| | ) | |
| v. | ) | CR 18-292 |
| | ) | |
| ROBERT BOWERS | ) | |
| | ) | |

## OPINION AND ORDER

### Synopsis

The Defendant has filed a Motion to Suppress Evidence Seized During the Search of Records Associated Geolocation Data and Email Address ("Motion to Suppress No. 13"). [ECF 300 (Redacted motion), 308 (Sealed Motion), 318 (Exhibit)]. The Government has filed a Response [ECF 348 (Redacted Response); 359 (Sealed Response)]. Defendant has replied [ECF 382 (Redacted Reply); 394 (Sealed Reply)], and the Government has filed a Sur-Reply. [ECF 401]. For the following reasons, Defendant's Motion will be denied.[1]

### Analysis

Although raised in one Motion, the Defendant seeks suppression of evidence seized during searches of records associated with two accounts: (1) a Hyundai Blue Link account; and (2) the email address "onedingo@comcast.net." The Defendant maintains that the Government obtained search warrants for each search in violation of the Fourth Amendment.

[1] The Defendant insists that an evidentiary hearing is required in order to resolve disputed issues of fact. I disagree. A hearing is required on a suppression motion if it raises issues of fact material to the resolution of the defendant's constitutional challenge. United States v. Hines, 628 F.3d 101, 105 (3d Cir. 2010). The defense bears the burden of demonstrating entitlement to a hearing. United States v. Stevenson, No. 16-189, 2019 U.S. Dist. LEXIS 172592, at *4 (W.D. Pa. Oct. 4, 2019). Because no material facts are at issue here, no hearing is required on the Motion at bar.

(1) Hyundai Blue Link Account

On the date of the crime at issue, the Defendant is alleged to have driven a 2016 Hyundai Sonata and parked it just outside the Tree of Life Synagogue. Investigators confirmed that the car belonged to the Defendant and that it was equipped with the Hyundai Blue Link Connected Car Service ("Hyundai Blue Link"). The Hyundai Blue Link provides numerous features, several of which – including accessing, maintaining, and monitoring a vehicle's geolocation data – were of interest to the investigators. On January 20, 2020, the Government sought and obtained authorization to seize records associated with the Hyundai Blue Link account. Hyundai returned the executed search warrant and provided account records dating back to October 2015, a copy of the Blue Link manual, and account-related communications between Hyundai and the Defendant dating back to March 2016. No geolocation information was returned. Because no geolocation information was returned, the only information at issue relates to the subscriber account information.

The Defendant challenges the search warrant as overbroad and lacking particularity. Specifically, as to the breadth of the warrant, the Defendant argues that because the warrant did not include a date restriction, it permitted the Government to seize all records from the date the account was activated through the present time. While conceding that that there is probable cause for a search of the account for the date of the crime at issue, he contends that the affidavit does not establish a link to a crime for any other date. In terms of his particularity challenge, the Defendant urges that the warrant does not tie the search to a particular crime or criminal behavior. While acknowledging that the supporting affidavit ties the search to the particular crimes at

issue, the Defendant insists that because the supporting affidavit is not incorporated by reference into the warrant or attachments thereto, the supporting affidavit is irrelevant.

Neither challenge is persuasive. I agree with the Government that the Defendant lacks standing to assert a Fourth Amendment challenge. "A search does not occur for Fourth Amendment purposes unless the individual challenging the search 'manifested a subjective expectation of privacy' in the object searched, and society recognizes that expectation as reasonable." *United States v. Brewer*, 708 Fed. Appx. 96, 99 (3d Cir. 2017), *citing, Kyllo v. United States*, 533 U.S. 27, 33, 121 S. Ct. 2038 (2001). The Defendant does not have a reasonable expectation of privacy in the information in the Hyundai Blue Link records. As the Tenth Circuit recognized in *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008), subscriber information provided to an internet provider is not protected under the Fourth Amendment because there can be no reasonable expectation of privacy in information that is voluntarily transmitted to third-party providers. *See also, United States v. Christie*, 624 F.3d 558, 573 (3d Cir. 2010) ("no reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including ISPs."). Similarly, there is "no reasonable expectation of privacy in telephone subscriber information and records or flight and ticketing information." *United States v. Brooks*, Crim. No. 19-3562, 2020 WL 7705649, at * 3 (3d Cir. Dec. 29, 2020 (citations omitted). Significantly, the Defendant offers no response to the Government's standing challenge in this respect. Rather, the Defendant's argument as to "standing" is directed solely to his Comcast

email account. Consequently, the Motion to Suppress Evidence associated with the Hyundai Blue Link account is denied.[2]

(2) Comcast Email Account

With respect to the Comcast email account, the Defendant asserts that the affidavit submitted in support of the search warrant failed to establish probable cause that a search would yield evidence of criminal activity. More specifically, he urges that the affidavit did not establish a "nexus" between the criminal activity and the email account (onedingo@comcast.net).[3] Instead, the affidavit establishes only that the email account was used for receipt of correspondence from the internet service provider Tucows/Hover/eNom and, he reasons, the Government has not supplied any facts suggesting that he used this email account in any other manner. Consequently, the Defendant concludes, it is not reasonable to infer that the Defendant may also have used this email account to communicate his animus toward other races and religions. Assuming, for purposes of argument only, that the Defendant has any privacy interest in the Comcast account, I reject his probable cause challenge.

---

[2] Even if the Defendant had standing to challenge the Hyundai Blue Link, I would decline to suppress the results of the search. The warrant is not overbroad. "Probable cause is a 'practical, nontechnical concept.'" *United States v. Leveto*, 343 F. Supp.2d 434, 448 (W.D. Pa. 2004), *quoting, Illinois v. Gates*, 462 U.S. 213, 230, 103 S. Ct. 2317 (1983). Although lacking specific dates, the car at issue was a 2016 model year with the account being activated in October 2015. Any search would not predate that time frame. Further, based upon the assertions in the affidavit and the experience of the affiant, I find no error with respect to the magistrate judge's conclusion that a reasonable probability existed that evidence of the crimes charged would be found in the Blue link account during the time frame at issue. Nor does the warrant lack in particularity. The failure to cite the charges being investigated is not fatal. "[T]here is no *per se* requirement that a search warrant describe the criminal activity alleged." *United States v. Kofsky*, Crim. No. 6-392, 2007 WL 2480971, at * 16 (E.D. Pa. Aug. 28, 2007). Rather, reference to alleged criminal activity in a search warrant is relevant where an otherwise "general warrant" fails to confine the discretion of the executing officers, such as by including a list of items to be seized. Here, the warrant is not "general" in nature. Rather, the information sought is necessarily confined to a Blue Link account and the limited information it holds.

[3] The Defendant concedes that the Government has alleged a nexus between the other email address associated with him (RBowers@onedingo.com) and the criminal activity insofar as he is said to have used that email address to communicate his animus towards other religions and races.

The Fourth Amendment to the Constitution provides in part that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *U.S. CONST., amend. IV.* "Probable cause" is the threshold requirement for the issuance of a warrant. The Supreme Court directs that courts assess the existence of probable cause based upon a "totality-of-the-circumstances" analysis. The issuing magistrate must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before her, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238, 103 S. Ct. 2317 (1983). Accordingly, our Court of Appeals has cautioned against "'overly compartmentaliz[ing]' the determination of probable cause." *United States v. Yusuf,* 461 F.3d 374, 390 (3d Cir. 2006) (citations omitted). Instead, the Court must "consider the cumulative weight of the information set forth by the investigating officer in connection with reasonable inferences that the officer is permitted to make based upon the officer's specialized training and experiences." *Yusuf*, 461 F.3d at 390, *citing, United States v. Arvizu*, 534 U.S. 266, 275, 122 S. Ct. 744 (2002). Probable cause is a "fluid concept" and turns "on the assessment of probabilities in particular factual contexts not readily, or even usefully, reduced to a neat set of legal rules." *Gates*, 462 U.S. at 232, 103 S. Ct. 2317. "[D]irect evidence linking the place to be searched to the crime is not required for the issuance of a search warrant." *United States v. Hodge*, 246 F.3d 301, 305 (3d Cir. 2001) (internal quotation marks omitted).[4]

[4] "Although every affidavit ideally would contain direct evidence linking the crime with the place to be searched, a magistrate [judge] may issue a search warrant even without direct evidence. Probable cause

Reviewing courts apply a deferential standard to challenges to the issuance of a warrant. *See United States v. Stearn*, 597 F.3d 540, 554 (3d Cir. 2010). "[O]ur role is not to make our own assessment as to whether probable cause existed. Rather, we are constrained to determine only whether the affidavit provides a sufficient basis for the decision the magistrate judge actually made." *United States v. Jones*, 99 F.2d 1051, 1057 (3d Cir. 1993). "If a substantial basis exists to support the magistrate [judge's] probable cause finding, [the Court] must uphold that finding even if a 'different magistrate judge might have found the affidavit insufficient to support a warrant.'" *Stearn*, 597 F.3d at 554, *quoting, United States v. Conley*, 4 F.3d 1200, 1205 (3d Cir. 1993). Of course, a reviewing court does not merely "rubber stamp a magistrate's conclusions." *United States v. Whitner*, 219 F.3d 289, 296 (3d Cir. 2000) (citations omitted). Yet, "doubtful or marginal cases in this area should be largely determined by the preference to be accorded to warrants." *Gates*, 462 U.S. at 237 n. 10, 103 S. Ct. 2317 (citation and quotations omitted).

Employing the appropriate deferential standard, I find that the search warrant application and accompanying affidavit provided the issuing magistrate judge with a substantial basis for concluding that a search of the Comcast email account would elicit evidence of the crimes at issue. The Affiant explains that he has received specialized training in computer crime investigations and criminal cyber investigations and that the information set forth in the Affidavit is based upon his own personal investigation, observations, and knowledge as well as upon the investigations, observations, and

---

can be, and often is, inferred from 'the type of crime, the nature of the items sought, the suspect's opportunity for concealment and normal inferences about where a criminal might hide [evidence].' *United States v. Jones*, 994 F.2d 1051, 1056 (3d Cir. 1993) (citations and quotation marks omitted).

knowledge of other law enforcement officers with whom he discussed the case. The Affidavit details the Defendant's entry to the Tree of Life Synagogue at a day and time when congregants gathered to observe religious services. [ECF 318, ¶ 5, 6] The Affiant explains that the Defendant armed himself with multiple weapons, shot and killed eleven individuals, and wounded others, including law enforcement officers. [*Id.* at ¶ 7]. He further states the Defendant made audible statements regarding genocide, a desire to kill Jewish people, and that Jewish people needed to die; he stated to a law enforcement officer, "I just want to kill Jews." [*Id.* at ¶ 8]. He establishes that the Defendant used electronic communications and social media as a means of communicating his views of racial and religious animus. [Id. at ¶ 18-27]. The Affiant also established that the Defendant used email to communicate with his relatives. In particular, the Defendant's mother stated that the Defendant sent her videos and news items via emails that demonstrated a bias against Jewish people. [Id. at ¶ 21]. The Affiant further represented that the Defendant was the owner of the domain name "onedingo.com".[5] A separate email account (warroom@onedingo.com) was associated with a website (www.warroom.com) which hosted information associated with a conservative radio host's talk show. Apparently, the Defendant acted as the show's archiver and solicited sponsors for server space using that email address. [Id. ¶ at 22]. Law enforcement also obtained search warrants for two of the Defendant's other email accounts (ODGPhone@gmail.com and onedingo@gmail.com) only to learn that both accounts, and much of the communications and data, had been deleted. [Id. at ¶ 30]. Similarly, law enforcement found an encrypted LG phone on the Defendant at the scene

[5] The domain name was registered with Tucows, and its subsidiaries Hover and eNom.

of the crime and a home-built computer at his residence. The LG phone was highly encrypted and the home computer was equipped with a sophisticated destruct command. [Id. at ¶ 31-32].

Viewed as a whole, considering the totality of the circumstances, and giving appropriate deference, I find that the magistrate judge made reasonable inferences in this instance. There was a substantial basis for the magistrate judge to conclude that there was probable cause that evidence of the charged crimes as listed in the Application for Search Warrant would be found in the Comcast email account. The Affidavit contained sufficient information indicating that the Defendant demonstrated racial / religious animus towards Jewish people; that he had communicated such animus in the past via email, social media, or other means of electronic communication; and that the information stored in the Comcast records might contain evidence of such animus and / or of the Defendant's planning or premeditation. In so finding, I reject the Defendant's suggestion that the magistrate judge made unreasonable inferential leaps in finding probable cause.

In the alternative, assuming for purposes of argument only that the magistrate judge erred in issuing the warrant, I find that the good faith doctrine applies. Consequently, the suppression of the evidence is not warranted. *Herring v. United States,* 555 U.S. 135, 137 (2009) ("[S]uppression is not an automatic consequence of a Fourth Amendment violation."). The goal of the exclusionary rule is to deter Fourth Amendment violations. *Id.* at 139-140*; see also, United States v. Werdene,* 883 F.3d 204, 215 (3d Cir. 2018). Exclusion is a "last resort, not our first impulse." *Id.* at 140. It is applied only in those "'unusual cases' where it may achieve its 'remedial objectives': to

appreciably deter unreasonable searches and seizures by law enforcement officers." *United States v. Caesar*, Crim. No. 19-3961, 2021 WL 2559471, at * 6 (3d Cir. June 23, 2021), *citing United States v. Leon*, 468 U.S. 897, 908, 104 S.Ct. 3405 (1984). Accordingly, if officers acted with an "objectively reasonable good-faith belief that their conduct [was] lawful or when their conduct involve[d] only simple, isolated negligence," there is no deterrent effect justifying exclusion of evidence. *United States v. Katzin,* 769 F.3d 163, 171 (3d Cir. 2013). The good faith exception inquiry rests on "'the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal' in light of 'all of the circumstances.'" *United States v. Horton,* 863 F.3d 1041, 1051 (8th Cir. 2017), *quoting, Herring*, 555 U.S. at 145. Simple, isolated, or negligent conduct does not warrant suppression. Rather, "[t]o trigger the exclusionary rule, law enforcement conduct must be 'deliberate, reckless, or grossly negligent,' or involve 'recurring or systemic negligence.'" *Caesar*, 2021 WL 2559471, at * 7 (citations omitted).

In this case, there is no suggestion of deliberate, reckless, or grossly negligent disregard of the Fourth Amendment. I find suppression would have no appreciable deterrent effect because a reasonable officer would not have known that the detailed and limiting list of items be seized in the warrant was invalid despite the magistrate judge's authorization. Moreover, contrary to the Defendant's position, and as set forth above, the allegations set forth in the Application provides a substantial basis to establish probable cause. Therefore, I find suppression would have no appreciable deterrent effect because a reasonable officer would not have known that the detailed and limiting list of items to be seized in the warrant was "so deficient" despite the magistrate judge's authorization.

Consequently, even if there was a Fourth Amendment violation, I find the good faith exception to the exclusionary rule applies and suppression is not warranted.[6]

**Conclusion**

Based on the foregoing, I find no Fourth Amendment violations. Therefore, the Defendant's Motion to Suppress Evidence Seized During Search of Records Associated With Geolocation Data and Email Address (Motion to Suppress No. 13) shall be denied.

An appropriate order shall follow.

July 8, 2021

BY THE COURT:

Donetta W. Ambrose
United States Senior District Judge

[6] Given my holding, I need not reach the Government's "inevitable discovery" argument.

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

| | | |
|---|---|---|
| UNITED STATES | ) | |
| | ) | |
| | ) | |
| -vs- | ) | CR 18-292 |
| | ) | |
| ROBERT BOWERS, | ) | |
| | ) | |
| Defendant. | ) | |

AMBROSE, Senior District Judge.

**ORDER OF COURT**

AND NOW, this 8th day of July, 2021, it is hereby ORDERED that the Defendant's Motion to Suppress No. 13 (ECF Nos. 300, 308) is DENIED.

BY THE COURT:

Donetta W. Ambrose
United States Senior District Judge